Lari Oranen

PALVELUNESTOHYÖKKÄYKSET JA NIILTÄ SUOJAUTUMINEN

Opinnäytetyö
Tietotekniikan koulutusohjelma

Toukokuu 2015

MAMK
University of Applied Sciences

KUVAILULEHTI

MAMK University of Applied Sciences	**Opinnäytetyön päivämäärä** 28.5.2015
Tekijä(t) Lari Oranen	**Koulutusohjelma ja suuntautuminen** Tietotekniikan koulutusohjelma

Nimeke

Palvelunestohyökkäykset ja niiltä suojautuminen

Tiivistelmä

Palvelunestohyökkäykset ovat viime vuosien aikana saaneet runsaasti palstatilaa, varsinkin pankkeja vastaan tehdyt hyökkäykset ovat herättäneet suurta huomiota. Opinnäytetyön tavoitteena oli tutkia palvelunestohyökkäyksien anatomiaa ja selvittää, kuinka niiltä voi suojautua ja kuinka hyökkäyksen uhriksi joutunut voi vähentää vahinkoja.

Työssä käydään läpi protokollat ja verkon osat, joihin suurin osa palvelunestohyökkäyksistä perustuu sekä ihmisryhmät, jotka hyökkäyksiä tekevät, heidän motivaatiot ja yleisimmät hyökkäysten uhrit. Kattavan kuvan muodostus palvelunestohyökkäyksistä auttaa puolustamisen muodostamisessa niitä vastaan tietoverkoissa.

Hyökkäysten tutkimisen jälkeen esitellään keinoja, joilla välttää hyökkäyksen uhriksi joutumista. Palvelunestohyökkäysten tapauksessa on tärkeämpää välttää iskuja ja tehdä itsestä liian monimutkaisen maali. Ennakkoon varautuminen on välttämätöntä, sillä käynnissä olevan palvelunestohyökkäyksen tuhojen lieventäminen on yleensä todella hankalaa.

Hyökkäyksen uhriksi joutuessa työssä tärkeimmäksi toimeksi päätettiin hajauttaminen. Volyymi- ja ohjelmistotason hyökkäyksillä saadaan usein kohde toimintakyvyttömäksi, verkon ylläpidon kannalta on tärkeää hajauttaa tärkeitä palveluita eri osoitteisiin ja varmistaa, ettei hyökkäys kaada kaikkia palveluita kerralla.

Asiasanat (avainsanat)

DoS, DDos, palvelunestohyökkäykset, tietoturva, hajauttaminen

Sivumäärä 33	**Kieli** Suomi

Huomautus (huomautukset liitteistä)

Ohjaavan opettajan nimi Matti Koivisto	**Opinnäytetyön toimeksiantaja**

DESCRIPTION

MAMK University of Applied Sciences	**Date of the bachelor's thesis** 28.5.2015
Author(s) Lari Oranen	**Degree programme and option** Information technology

Name of the bachelor's thesis

Denial of Service attacks and protecting against them

Abstract

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks have gained a lot of attention in past few years, especially attacks made against banks. The purpose of this study was to gain information on the anatomy of DoS attacks and find out how to protect from them or to minimize the damage if an attack happened.

The study explores protocols and network components that most DoS attacks base their function on and found out who orchestrate these attacks, what their motivation is and how they choose their victims. Studying the background of DoS attacks helps understanding them and therefore protecting the network against attacks.

After the theory part the study presented means to prevent one from becoming a victim of an attack. In DoS attacks it is more important to avoid the attacks altogether and make to yourself too complicated a target for an attack. Prevention and preparation is essential as mitigating an undergoing DoS attack is usually very troublesome.

Study concluded that if you became a victim of a DoS attack the most important thing was spreading network resources, load balancing and redundancy. Volume and application layer attacks often succeed in crippling their target services or devices. Therefore it's important for constant network uptime to spread services to different addresses and make sure one attack does not crash all services at once.

Subject headings, (keywords)

DoS, DDoS, IT security, load balancing

Pages 33	**Language** Finnish

Remarks, notes on appendices

Tutor Matti Koivisto	**Bachelor's thesis assigned by**

SISÄLTÖ

1 JOHDANTO 1

2 TIETOVERKON TOIMINTA 2

2.1 IP-paketit 2

2.1.1 IP-osoitteisto 2

2.1.2 IP-paketin sisältö 3

2.2 TCP-protokolla 4

2.3 UDP-protokolla 5

3 PALVELUNESTOHYÖKKÄYKSET 5

3.1 Yleistä 6

3.2 Tekijät, kohteet ja motiivit 8

3.2.1 Ammattimaiset tekijät 8

3.2.2 Yksityishenkilöt 9

4 YLEISIMMÄT HYÖKKÄYSTAVAT 11

4.1 Protokollatason ja volyymiperäiset hyökkäystyylit 11

4.1.1 UDP fragment ja UDP flood 11

4.1.2 TCP SYN flood 13

4.1.3 Heijastushyökkäykset 14

4.1.4 Ping of Death ja ICMP 16

4.2 Ohjelmistotason palvelunestohyökkäykset 16

4.2.1 Ohjelmistot 17

5 HYÖKKÄYKSILTÄ SUOJAUTUMINEN JA VAHINKOJEN MINIMOINTI 18

5.1 Palomuurit 19

5.2 Puolustus pilvessä 21

5.3 IDS / IPS 22

5.3.1 IDS 23

5.3.2 IPS 24

5.4 Hajauttaminen 25

5.5 Yksityishenkilöiden suojautuminen 27

6 YHTEENVETO 28

LÄHTEET 31

LYHENTEET

DoS: Denial of Service, palvelunestohyökkäys.

DDoS: Distributed Denial of Service, hajautettu palvelinestohyökkäys.

IP: Internet Protocol, internet-protokolla.

NAT: Network Address Translation, verkon osoitteenmuutos.

DNS: Domain Name Service, verkon nimipalvelujärjestelmä.

TCP: Transmission Control Protocol, tietoliikenneprotokolla.

UDP: User Datagram Protocol, yhteydetön tietoliikenneprotokolla.

NTP: Network Time Protocol, verkon aikapalvelun protokolla.

ICMP: Internet Control Message Protocol, kontrolliprotokolla verkon pienille viesteille.

SNMP: Simple Network Management Protocol, verkon hallintaan tarkoitettu protokolla.

HTTP: Hypertext Transfer Protocol, selainten ja internet-sivustojen tiedonsiirtoon käyttämä protokolla.

LOIC: Low Orbit Ion Cannon, palvelunestohyökkäykseen käytetty yksinkertainen ohjelma.

VPN: Virtual Private Network, kahden laitteen muodostama salattu tunneli verkon yli.

VPS: Virtual Private Server, vuokrattava virtuaalipalvelin.

IDS: Intrusion Detection System, verkkoliikenteen monitorointia ja hälytyksiä epäilyttävästä toiminnasta antava laite.

IPS: Intrusion Preventation System, verkkoliikennettä tarkkaileva laite joka hälyttää epäilyttävästä toiminnasta ja torjuu sitä.

1 JOHDANTO

Nykyisin monet organisaatiot ovat siirtäneet tiedonhallinnan suurilta osin, jotkut täydellisesti verkkoon. Tietoverkot aiheuttavat tietoturvariskejä ja jatkuvaa mukautumista vallitsevaan tietoturvatilanteeseen. Turvan lisäksi organisaatio odottaa tietoverkon käytettävyyden olevan lähellä sataa prosenttia eli verkon pitäisi olla aina ylhäällä. Vähäinenkin verkon alhaalla olo saattaa yrityksessä johtaa mittavaan rahan menetykseen. Valitettavasti palvelunestohyökkäykset tähtäävät juuri verkkojen alas ajoon, mikä tekee niihin valmistautumisesta ja suojautumisesta ensiarvoisen tärkeää.

Tutkin työssä palvelunestohyökkäysten taustat, tavoitteena ymmärtää hyökkäysten kulku, hyökkäysten tekijöiden motiivit ja uhrien valinta. Taustan ymmärtäminen helpottaa vastatoimien eli suojautumisen ja hyökkäyksen uhrin vahinkojen minimoimisen suunnittelua.

Työn alussa pureudutaan perusasioihin eli verkon yleisimpien protokollien toimintoihin. Nämä protokollat ovat isossa roolissa suurimmassa osassa palvelunestohyökkäyksistä. Protokollat ovat tietotekniikan mittareilla ikivanhoja eikä niitä ole suunniteltu tietoturvaa ajatellen, mikä on johtanut niiden monenlaiseen väärinkäyttöön.

Seuraavaksi läpi käydään palvelunestohyökkäykset ilmiönä ja pureudutaan hyökkäyksiä tekeviin tahoihin ja heidän motivaatioihinsa. Palvelunestohyökkäyksiä tapahtuu sekä valtiollisella tasolla että täysin amatöörien yksityishenkilöiden taholta ja kohde määräytyy yleensä tekijän mukaan, esimerkiksi yksityishenkilöiden hyökkäyksien motivaatio on yleensä kiusanteko ja huomio.

Tämän jälkeen pureudutaan tarkemmin yleisimpiin hyökkäystyyleihin ja käydään läpi kuinka ne toimivat ja kuinka hyökkääjät ne toteuttavat. Kun melko kattava kuva hyökkäyksistä on muodostettu, viimeinen luku keskittyy hyökkäyksiltä etukäteen suojautumiseen. Aina valmistautuminen ei kuitenkaan riitä ja tapoja vähentää hyökkäyksen vahinkoja esitellään myös.

2 TIETOVERKON TOIMINTA

Suurin osa palvelunestohyökkäyksistä perustuu tietoverkon perustoimintoihin ja verkon kulmakivet, kuten IP-, TCP- ja UDP-protokollat ovat pääosissa yli puolista hyökkäyksistä. Yleisesti tietoverkon toimintaa esitellään seitsemän tason OSI-mallissa, jossa jokaisella tasolla vaikuttavat protokollat huolehtivat tiedonsiirrosta verkon välillä. Luvussa tarkastellaan alemman kerroksen protokollia, joilla määritetään kuinka tieto siirretään paikasta toiseen, ylemmät kerrokset keskittyvät itse tiedon sisältöön.

2.1 IP-paketit

Tieto liikkuu verkossa paketeissa. Näiden pakettien peruskivi on IP-paketti, kaikki verkon yli liikkuva tieto sisältää IP-protokollan määrittelemät perustiedot. IP-protokollan tärkein sisältö on osoitetieto, eli paketit sisältävät lähtöpaikan ja määränpään.

2.1.1 IP-osoitteisto

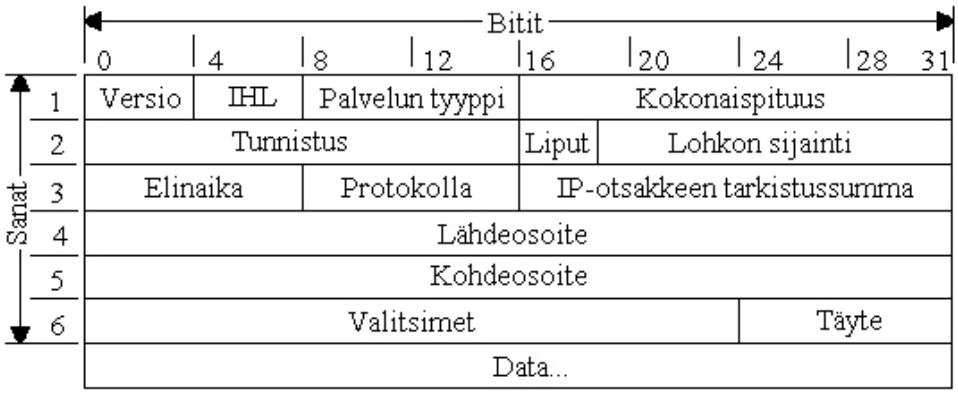
IP-paketit löytävät perille sen oman osoitesysteeminsä ansiosta. Nykyisin käytössä oleva IPv4 käyttää 32-bittistä osoitteistoa, tämä osoite jaetaan jokaiselle julkiseen verkkoon liittyvälle laitteelle. Käytännössä tämä tarkoittaa lukusarjaa, joka on jaettu neljään osaan, jokaisen osan ollessa väliltä 0-255. Esimerkkiosoitteena 125.255.188.144. IPv4:n mahdollistaessa vain 4 294 967 296 osoitetta. Tämän vuoksi internetissä ollaan siirtymässä IP:n kuudenteen versioon jonka pidempi, 128-bittinen osoitteisto mahdollistaa valtavan määrän osoitteita, yli 340 sekstiljoonaa (Goldman 2012).

IPv4:n osoitepulaa hoidetaan NAT:lla (Network Address Translation) eli osoitteenmuunnoksella, jolloin sisäverkon laitteille voi jakaa minkä osoitteen tahansa, yhteydessä ulkomaailmaan ne käyttävät vain yhtä IP-osoitetta ja päätteet erotellaan porttinumeroilla, esimerkiksi sisäverkossa kone voidaan tunnistaa 192.168.1.1 -osoitteella mutta ulkomaailmaan sen osoite on 165.192.1.1:2000, vieressä olevan

koneen osoitteen ollessa vaikka 165.192.1.1:2027. NAT:n lisäksi toinen yleinen IP-osoitteeseen vaikuttava tekniikka on DNS (Domain Name System), nimipalvelu jossa numeraalinen IP-osoite voidaan muuttaa tekstiksi joka helpottaa osoitteiden muistamista. Esimerkiksi www.google.fi -osoitteen takaa paljastuu IP-osoite 74.125.71.94. Osoitemuunnoksen ja nimipalvelun yksityiskohtiin voi tutustua tarkemmin Internet-dokumenteissa RFC 1631 (Egevang & Francis 1994) ja RFC 1035 (Mockapetris 1987).

2.1.2 IP-paketin sisältö

Kuvassa 1 esitetty IP-paketti sisältää paljon eri osia, mutta tärkeimmiksi voi mainita itse liikuteltava data, paketin lähde- ja kohdeosoite, paketin elinaika, tarkistussumma ja fragmentin tunnus ja paikka.



KUVA 1. IP-paketin rakenne (TCP/IP-protokolla 2001)

Joskus lähetettävä paketti on niin iso, että se on pilkottava, eli se fragmentoituu. Tällöin paketille määrätään erikseen sen tunnus ja paikka paketissa, jotta paketti voidaan taas kasata kohteessa kaikkien fragmenttien saapuessa perille.

Paketin elinajalla määritetään, kuinka monta kertaa paketti voi siirtyä eri verkon laitteiden välillä. Tällä varmistetaan, ettei paketti jää pyörimään verkossa ikuisesti, jos jonkinlainen virhe sattuu. Paketille annetaan elinaika väliltä 1 ja 255 ja aina kun se siirtyy laitteesta toiseen, vähennetään elinajasta yksi. Kun elinaika saavuttaa nollan,

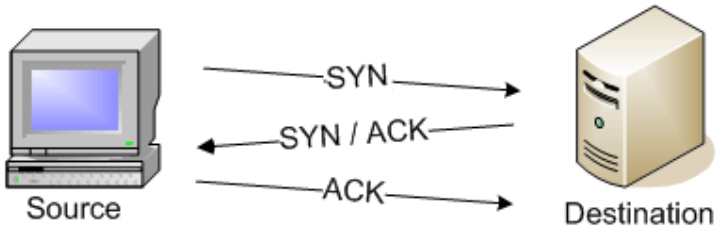
paketti pudotetaan, eli sitä silloin käsittelevä laite poistaa sen. Tarkistussummalla katsotaan, ettei paketti ole muuttunut matkan aikana virheiden takia.

2.2 TCP-protokolla

IP-paketti on verkon kulmakivi, mutta suurin osa itse liikenteestä käyttää jotain ylemmän kerroksen protokollaa sen lisäksi. Protokollat lisäävät IP-pakettiin oman sisältönsä. Näistä protokollista ylivoimaisesti käytetyin on TCP. TCP on määritelty yksityiskohtaisesti Internet-dokumentissa RFC 793 (Information Sciences Institute, 1981). TCP lisää IP-pakettiin paketin lähetys- ja kohdeportit. Suurin osa käytetyimmistä internetpalveluista käyttää jotain TCP-porttia, esimerkkeinä http:n (verkkosivut) portti 80, tai tiedostosiirtopalvelun portti 21. Eli ottaessa yhteyden www.google.fi:n, avaat TCP-yhteyden osoitteeseen 74.125.71.94:80.

TCP:n käytössä isoin etu on sen virheenkestokyky. Jos TCP:n paketit häviävät matkalla tai pakettien järjestysnumerot menevät sekaisin, se pyytää lähettäjää uusimaan paketin toimituksen. TCP:tä käyttävä ohjelma saa paketin vasta, kun protokolla kasannut sen valmiiksi, mikä saattaa johtaa hitauteen jos verkossa tapahtuu paljon virheitä esimerkiksi kuormituksen takia ja hitautensa takia TCP onkin käyttökelvoton esimerkiksi verkkopuheluiden hoitamiseen.

TCP:tä käytettäessä pääte varaa palvelimelta oman porttinsa liikenteen ajaksi. Tämän takia TCP käyttää omanlaista kättely-systeemiä yhteyden avaamiseksi ja sulkemiseksi. Yhteys pitää olla auki tai se pitää jokaisen paketin kohdalla. Kättelyssä palvelua aikova pääte lähettää palvelimelle SYN-viestin eli pyytää lupaa yhteyden aloittamiseksi. Palvelin vastaa tähän SYN-ACK-viestillä eli antaa luvan yhteyden muodostamiseen. Tämän jälkeen päätteen on vielä lähetettävä ACK-viesti, joka kuittaa luvan saaduksi ja vasta sen jälkeen yhteys voidaan muodostaa ja paketti lähtee liikkeelle.



KUVA 2. TCP-kättely (Messer)

Kättely hidastaa yhteyttä mutta varmistaa että paketit varmasti liikkuvat oikeiden kohteiden välillä. Jos yhteydessä tapahtuu virhe ja esimerkiksi SYN-ACK-viesti ei ikinä saavu, lähettää pääte uuden SYN-viestin kunnes kaikki toimii odotetusti. Kun pakettienvaihto lopetetaan, portti suljetaan samantyylisellä systeemillä, lopetuksessa tosin myös palvelin kysyy luvan lopettamiseen (Transmission Control Protocol 2015).

2.3 UDP-protokolla

Jo vuonna 1980 RFC 768:ssä (Postel, 1980) määritetty UDP-protokolla on TCP:n jälkeen käytetyimpiä protokollia. Samoin kuin TCP:ssä, myös UDP-paketit sisältävät osoitteiden lisäksi lähetys- ja kohdeportit, esimerkiksi NTP (Network Time Protocol) eli kellonaikapalvelu käyttää UDP-porttia 123. Muuten UDP-protokolla on todella riisuttu. Se ei käytä TCP:n kättelysysteemiä, paketin saapumista perille ei varmisteta, siinä ei tarkisteta mahdollisten duplikaattien saapumista eikä yhteyden lopettamisesta sovita erikseen.

Näillä puutteilla saavutetaan nopeus ja vähäisempi verkon kuormitus kuin TCP:llä, ja UDP:tä käytetäänkin yleensä nopeaa yhdistämistä ja tiedonsiirtoa vaativissa palveluissa, kuten nettipuheluissa, peleissä ja videon suoratoistossa. Esimerkiksi nettipuhelussa ei ole aikaa lähettää pakettia uudestaan, jos se sattuu putoamaan matkalla tai sen saapuminen on hidastunut, puhelun on jatkuttava häiriöstä huolimatta.

3 PALVELUNESTOHYÖKKÄYKSET

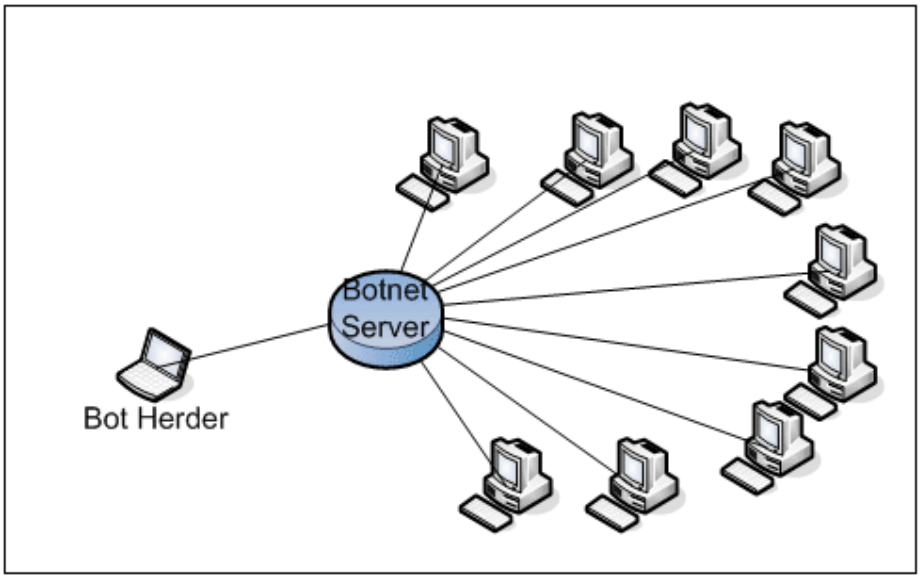
Palvelunestohyökkäykset eivät ole organisaation tietoturvauhkana uusi asia. Varsinkin viime vuosina hyökkäysten määrät ovat kuitenkin lisääntyneet niin paljon, että asiaan on alettu suhtautua uudella vakavuudella tietoturvan kannalta. Määrään on vaikuttanut monia tekijöitä, kuten yksityishenkilöiden verkkoliittymien kaistan tasainen kasvu, joka on mahdollistanut entistä suuremman liikenteen luonnin kotioloista. Tai määrään on vaikuttanut jatkuvasti lisääntyvien verkossa tilattavien palvelunestohyökkäyspalveluiden määrä. Ja palvelunestoa on tutkittu ja kokeiltu kybersodankäynnin aseena. Yhtä kaikki, palvelunestohyökkäykset ovat nyt niin sanotusti pinnalla.

3.1 Yleistä

Kun internetiä aikoinaan suunniteltiin, ei ollut tarvetta keskittyä tietoturvaan, verkonhan oli tarkoitus tulla vain Yhdysvalloissa viranomaiskäyttöön. Suurin osa internetiä pyörittävistä protokollista on tietotekniikassa mitattuna antiikkisia, yli 30 vuotta vanhoja. Niinpä niitä on helppo väärinkäyttää ja valtaosa vanhoista protokollista on pääosassa palvelunestohyökkäyksissä. Palvelunestohyökkäyksestä käytetään yleensä lyhennettä DoS (Denial of Service) ja hajautetusta hyökkäyksestä lyhennettä DDoS (Distributed Denial of Service). DoS-hyökkäys tapahtuu yhdestä osoitteesta, hajautetussa hyökkäyksessä mukana olevia tietokoneita voi olla tuhansia ja eri maista.

Palvelunestohyökkäyksissä verkon komponenttien väärinkäytöllä on vain yksi tarkoitus, lamauttaa kohteen toiminta. Verkon yksi perusominaisuuksista on sen käytön helppous. Verkko on saavutettavissa vuorokauden ympäri ja mistä tahansa missä on yhteys saatavilla, tämän perusomaisuuden lamauttaminen tekee vaikutuksesta voimakkaan. Hyökkäyksessä pyritään lähtökohtaisesti estämään peruskäyttäjän pääsy palveluun, yleensä tukkimalla palvelun tiedonsiirtoyhteydet. Palvelun toimimattomuus on helppo huomata, hyökkäyksien ei ole tarkoituskaan olla salakavalia vaan mitä suuremman huomion hyökkäyksellä saa, sitä tyytyväisempi hyökkääjä yleensä on. Myös viime aikoina harvinaisempia, hitaampia DoS-hyökkäyksiä on. Näissä hyökkäys naamioidaan normaalina verkkoliikenteenä ja ylläpitäjä saattaa luulla että palveluun on vain normaalia isompi liikenne (Saarelainen 2014, 17).

Hajautettu hyökkäys tapahtuu yleensä haittaohjelmalla kaapattujen koneiden kautta. Hyökkäysten päämaat, Yhdysvallat ja Kiina ovat täynnä saastuneita, vanhoja ja tietoturvattomia tietokoneita jotka, käyttäjänsä tietämättä osallistuvat hyökkäyksiin. Pienistä puroista koostuu iso joki ja jopa 80 000 koneen verkko on havaittu yksittäisessä hyökkäyksessä (Glenny 2011, 179). Näiden bottiverkkojen vuokraus on yleistä, yksityishenkilökin voi tilata bottiverkon ylläpitäjältä hyökkäyksen haluamaansa kohteeseen ja maksaa hyökkäyksen keston perusteella, kiinnijäämisen mahdollisuuden ollessa todella pieni. Hyökkäyksen suorittamiseen sen toteuttaja tarvitsee vain kohdepalvelun tai tietokoneen IP-osoitteen, mikä tekee niiltä täydellisen suojautumisen mahdottomaksi, IP-osoitteenhan on oltava saatavilla verkon asiakkaille.



KUVA 3. Bottiverkko, palvelimella ohjaillaan saastuneita koneita (Woelk 2007)

Internetistä löytyy useita palveluja joilla pyritään esittämään reaaliajassa maailmalla tapahtuvia palvelunestohyökkäyksiä. Minuutin tarkkailun aikana Norse-kartalla(http://map.ipviking.com/) tapahtui noin 200 havaittua hyökkäystä, joista puolien lähtömaa oli joko Yhdysvallat tai Kiina. Nämä palvelutkaan eivät havaitse kaikkia hyökkäyksiä, joten oikeasti hyökkäysten määrä on vielä suurempi. Saarisen (2014, 20) mukaan vaikka hyökkäysten määrä jatkuvasti lisääntyykin, on niiden kesto lyhentynyt keskimäärin 32 tunnista 23 tuntiin.

3.2 Tekijät, kohteet ja motiivit

Palvelunestohyökkäysten tekijät löytyvät laajalta skaalalta. Yksinkertaisimmillaan hyökkääjä on yksityishenkilö, joka joko kotilaitteellaan tai tilatulla palvelulla häiritsee kohdetta, lähinnä huomiota ja vallantunnetta saadakseen. Periaate on usein sama kuin virusten ja matojen tehtailijoilla, hyökkäyksiä tehdään koska voidaan. Hyökkäysten skaalan toisessa päässä taas ovat sotilaalliset ja valtiolliset tahot, joiden hyökkäykset ovat voimakkaita, monimutkaisia ja niiden alkuperä lähes mahdoton selvittää.

3.2.1 Ammattimaiset tekijät

Palvelunestohyökkäykset ovat olleet valtioiden asearsenaalissa jo pidemmän aikaa. Georgian kriisi heinäkuussa 2008 koettiin vahva hyökkäys maan presidentin sivuja vastaan. Heinäkuun hyökkäyksen on päätelty olleen kenraaliharjoitus ennen elokuussa alkanutta aseellista konfliktia. Georgian ja Venäjän aloittaessa sotimisen, alkoi samalla armoton palvelunestohyökkäys Georgian valtiollisia internet-sivuja vastaan. Tämän hyökkäyksen katsotaan olleen ensimmäinen kerta kun aseelliseen konfliktiin liittyy myös kyberhyökkäyksiä (Markoff 2008). Kuten Viron patsaskiistassa, pitäviä todisteita Venäjän osallisuudesta hyökkäykseen ei ole.

Julkiset palvelut, pankit ja uutissivustot ovat usein hyökkäysten kohteena. Kuten aina IT-maailmassa, haitanteko saattaa olla vain kiusalla tehtyä tai hyökkääjän omien kykyjensä kokeilua. Lisäksi maiden kybersodankäynnin valmiuden kokeilua ei voi laskea pois vaihtoehdoista, välillä Suomessakin on koettu pankkien ja uutissivujen olevan samaan aikaan hyökkäysten kohteena mikä nostattaa kysymyksiä hyökkääjien ammattimaisuudesta.

Varsinkin pankit ovat kokeneet myös puhdasta verkkorikollisuutta, yhtiöitä yritetään kiristää maksamaan lunnaat tai palvelunestohyökkäys alkaa, maksaminen voi olla myös hyökkäyksen lopettamisen ehto kuten Suomessa alkuvuonna 2015 (Hallamaa 2015). Harvinaisessa kiristystapauksessa uudenvuoden vaihteessa kaksi miestä

aiheuttivat häiriöitä kolmen suomalaisen pankin verkkopalveluissa ja vaativat rahaa hyökkäyksen lopettamiseksi. Tapaus oli siinäkin mielessä Suomessa harvinainen, että kiristyksen tekijät saatiin kiinni ja asetettu syytteeseen.

Kiristyksen lisäksi hyökkäyksiä on käytetty savuverhoina, vuonna 2012 San Franciscolainen pankki joutui rajun DDoS-hyökkäyksen kohteeksi. Hyökkäyksellä oli hämäystä jonka turvin pankin järjestelmiin murtauduttiin ja onnistuttiin varastamaan noin 900 000 dollaria. Pankilla itsellään ei ollut hajuakaan ryöstöstä, se jäi kokonaan savuverhon taakse (Krebs 2013).

3.2.2 Yksityishenkilöt

Yksityishenkilö lähtee suorittamaan palvelunestohyökkäystä yleensä kahdesta syystä, kiusanteoksi tai osoittaakseen mielipiteensä eli aktivismina. Samat syyt pätevät kohteisiin, esimerkiksi poliitikko voi joutua lausunnosta eri mieltä olevien hyökkäyksen kohteeksi tai jollain tapaa kuuluisaa henkilöä häiritään kiusaksi.

Kolmas yksityishenkilöiden ryhmittymä on hakkeriryhmät, kuten Lizard squad (https://twitter.com/llzardsec). Nämä ryhmät häiritsevät eri kohteita omien sanojensa mukaan huvikseen ja voi hyvinkin olla että niiden jäsenistö koostuu henkilöistä joiden motiivi on vain kaaoksen luominen. Luultavasti kuuluisin hakkeriryhmän suorite oli kaataa vuoden 2014 joulupyhien aikaan Sonyn pelikonsoleiden verkot, mikä aiheutti laajaa mielipahaa lomapäiville osuneella ajoituksellaan.

Haktivisteiksi kutsutaan henkilöitä, jotka suorittavat aktivismia IT-maailmassa. Kuuluisin haktivisti-porukka on Anonymous-ryhmä jolla ei ole mitään yhteistä hierarkiaa. Siihen voi yksinkertaisesti liittyä, jos on samaa mieltä. Ryhmän kuuluisin mielenosoitus lienee WikiLeaksia ”tukenut” palvelunestohyökkäysten sarja, joka lähti alulle useiden yhtiöiden estäessä rahalahjoitukset WikiLeaksille omista systeemeistään. Muun muassa Visan, PayPalin ja Mastercardin palvelut kaadettiin tai saatiin hidastumaan kostona. Hyökkäyksellä oli vaikutusta, sen seurauksena PayPal

päätti vapauttaa WikiLeaksia tukeneen varainkeräysjärjestyksen tilin, joka oli aikaisemmin jäädytetty tuen takia (Operation Payback 2015).

Haktivistiryhmien toimiessa ilman kunnollista järjestyneisyyttä perustuu niiden hyökkäys yleensä volyymiin. Ryhmien käyttämät ohjelmistot eivät välttämättä suojaa hyökkääjän identiteettiä mitenkään mutta ryhmät luottavat massan voimaan, mukana on niin monesta maasta niin monta henkilöä, ettei kaikkia voida ottaa kiinni, yksittäinen hyökkääjä niin sanotusti hukkuu massaan.

Viime vuosien aikana elektroninen urheilu on kasvattanut voimakkaasti suosiotaan ja alalla on jo satoja ammattilaisia, pelaajia jotka tulevat toimeen tai jopa rikastuvat pelaamisella. Niin sanotun e-sportsin rinnalle on syntynyt uusi bisneksen muoto, streamaus. Streamauksessa eli suoralähetyksenä tapahtuva internet-show'ssa pelataan pelejä jopa sadoille tuhansille katsojille.

Sekä ammattilaispelaajat että streamaajat ovat suosineet erityisesti Skypeä sekä useaa muuta ohjelmistoa, joista tietoturva-aukkojen takia vuotaa käyttäjän IP-osoite maailmalle. Tästä syystä alan henkilöt ovat olleet hyökkäyksille helppoja maaleja ja kahden viime vuoden aikana hyökkäyksistä on tullut vitsaus.

Nimimerkillä PhantomL0rd toimiva streamaaja, oikealta nimeltä Jason Varga, on räkein esimerkki tapauksesta, jossa kiusalla suoritettu hyökkäys menee yli ja tekijöilläkään ei tuskin ollut enää käsitystä, kuinka vakavia rötöksiä tuli tehtyä. Perjantaina joulukuussa 2013 joku, kenties PhantomL0rdin fani tai show'sta ärsyyntynyt henkilö otti yhteyttä hakkeriryhmään DERP, kehottaen ryhmää hyökkäämään Vargan kimppuun ja ryhmä päätti toteuttaa pyynnön, omien sanojensa mukaan ”naurujen vuoksi”.

Vargan show kesti koko päivän ja sen aikana DERP kaatoi jokaisen pelin palvelimet, joita Varga yritti pelata. Näistä peleistä suosituimmalla League of Legendsillä on päivittäin jopa 30 miljoonaa pelaajaa(Riot Games 2015), ja muilla päivän aikana kaatuneilla peleilläkin käyttäjämäärät mitataan miljoonissa. Päivän aikana kaadettujen palvelimien omistavat peliyhtiöt menettivät siis huomattavia summia rahaa toiminnasta, joka pantiin alulle vitsin vuoksi. Samalla kiusan kohteeksi joutunut Varga

jopa yllytti DERP-ryhmää, Vargaa toiminta lähinnä huvitti. Huvi tosin loppui, kun DERP selvitti Vargan kotiosoitteen ja soittivat poliisit pidättämään miehen tekaistun rikoksen perusteella (Parkin 2014).

4 YLEISIMMÄT HYÖKKÄYSTAVAT

Palvelunestohyökkäyksen suoritustapoja löytyy todella paljon, käytännössä lähes jokaisessa vanhassa protokollassa on, tai on joskus ollut haavoittuvuus jota käyttää hyväksi. Lisäksi uusia haavoittuvuuksia keksitään kokoajan lisää, hyvänä esimerkkinä yli 30 vuotta käytössä ollut CHARGEN-protokolla, jonka palvelunestohyökkäyksiä mahdollistava haavoittuvuus on noussut suosioon vasta viime vuosina. Tapojen suuresta määrästä huolimatta luvussa esiteltävät hyökkäystyylit kattavat noin 90% kaikista hyökkäyksistä (Arbor Networks 2015).

4.1 Protokollatason ja volyymiperäiset hyökkäystyylit

Protokollatason ja volyymiperäisten hyökkäysten tarkoitus on joko tukkia uhrin kaista tai kaataa palvelin resurssien puutteeseen. Siksi niiden uhrin on yleensä helppo havaita, että hän on joutunut hyökkäyksen kohteeksi. Toisaalta ne ovat todella tehokkaita ja kohteen havaitessa hyökkäyksen voivat kaista tai verkon laitteet olla jo käyttökelvottomat ruuhkan vuoksi. Näissä hyökkäyksissä on myös tapana piilottaa hyökkääjän osoite, mikä vaikeuttaa vastuullisten kiinni saamista.

4.1.1 UDP fragment ja UDP flood

Globaalia verkkoliikennettä tarkkailevan Arbor Networksin mukaan UDP-pohjaiset DDoS-hyökkäykset kattavat noin 20–25% kaikista hyökkäyksistä (Arbor Networks 2015). Samantyylisiä fragmentointiin perustuvia hyökkäystyylejä on monenlaisia mutta niistä selvästi suosituin on UDP-protokollaan perustuva. Sekä fragment- että flood-yökkäys perustuu sekä protokollan heikkouksiin että volyymiin. UDP fragment-hyökkäys perustuu UDP-pakettien fragmentointiin eli ison paketin jakamisesta pienempiin osiin. Kohteelle lähetetään paljon isoja UDP-paketteja jotka, fragmentoituvat erittäin moneen osaan.

Fragmenttihyökkäys kuluttaa myös verkon kaistaa mutta sen pääkohde on vastaanottajan laskentateho. Fragmenttien kasaaminen ehjäksi paketiksi alkaa syödä kohteen resursseja, kunnes prosessorin tai muistin resurssit loppuvat ja kohde on käyttökelvoton (CAPEC 2014). Kaikissa UDP:tä käyttävissä palvelunestohyökkäyksissä on pääosissa UDP-paketin lähdeosoite, joka on helppo peukaloida, tällöin hyökkääjän identiteetti voidaan piilottaa sekä heijastushyökkäyksissä liikenne ohjata uhrille.

Flood-hyökkäyksessä käytetään hyödyksi UDP:n tapaa muodostaa yhteys. Koska TCP:n tapaista kättelysysteemiä ei ole, lähettäjän UDP-paketti otetaan aina vastaan. Floodauksessa hyökkääjä lähettää suuren määrän UDP-paketteja joiden kohdeportti on täysin satunnainen, suurin osa porteista ei sisällä mitään UDP:ta käyttävää palvelua. Kohde suorittaa kolme toimintoa saadessaan tälläisen paketin: tarkistaa käyttääkö mikään palvelu portissa UDP:ta, vahvistaa ettei käytä ja sen jälkeen lähettää ”ICMP Destination Unreachable” paketin (Incapsula 2015). ICMP Destination Unreachable ilmoittaa lähettäjälle, ettei alkuperäinen UDP-paketti saapunut minnekään. Kun kohde joutuu tekemään näitä tarkistuksia ja ICMP:n lähettämisiä liian monta samaan aikaan, eivät niin sanotut oikeat asiakkaat saa yhteyttä kohteeseen ja palvelut muuttuvat käyttökelvottomiksi.

Source IP	Source Port	Destination IP	Destination Port	Timestamp
192.168.27.37	1428	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1413	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1462	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1447	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1473	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1424	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1409	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1458	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1443	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1477	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1421	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1436	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1455	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1470	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1481	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1417	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1432	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1451	121.12.172.171	80	2009-04-20 13:40:21
192.168.27.37	1466	121.12.172.171	80	2009-04-20 13:40:21

KUVA 4. Esimerkki UDP floodista (UDP Flood 2002)

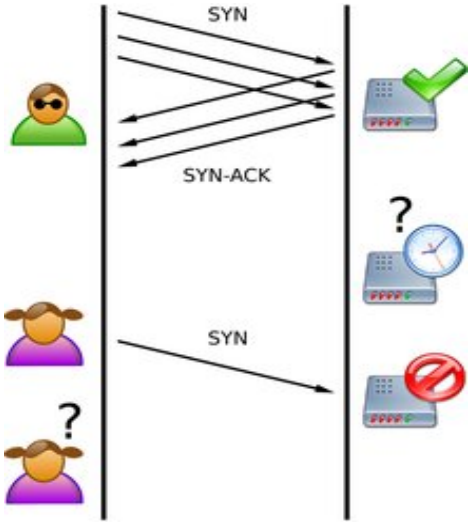
Kuvassa 4 esimerkki UDP floodista, vasemmalla pakettien lähtöosoite ja kohdeportti, keskellä palvelimen osoite ja oikealla aikatiedot. Palvelin saa sekunnissa yhdestä osoitteesta kymmeniä UDP-kyselyjä täysin satunnaisiin portteihin, ja jokainen kysely kohdistuu eri porttiin.

4.1.2 TCP SYN flood

TCP SYN flood on UDP floodin ohella käytetyin palvelunestomenetelmä. Se käyttää hyväksi TCP-protokollan tapaa avata yhteys asiakkaan ja palvelimen kanssa. TCP:n kättely vaatii 3 eri viestiä osapuolten kesken, kunnes asiakas voi avata yhteyden, yhteyden avaus alkaa asiakkaan lähettämällä SYN-viestillä johon palvelin tarjoaa SYN-ACK-vastauksen.

SYN floodissa hyökkääjä lähettää valtavan määrän SYN-viestejä palvelimelle mutta on säätänyt hyökkäävät koneensa torjumaan SYN ACK-vastauksen, näin ollen palvelin saa kyselyjä ja vastaa turhaan niin kauan kuin hyökkäys kestää. Tämä ei

yleensä täytä verkon kaistaa mutta rasittaa kohteen muistia ja prosessoria, estäen aitojen asiakkaiden yhteysyritykset, palvelin ei ehdi vastata muihin SYN-kyselyihin kuin hyökkääjän.



KUVA 5. SYN flood-hyökkäys (SYN flood 2015)

SYN flood-hyökkäys esitellään kuvassa 5. Violettipaitainen palvelun aito asiakas ei saa yhteyttä, koska hyökkääjä on tukkinut palvelun täysin.

4.1.3 Heijastushyökkäykset

Heijastushyökkäyksiä (tai peilaushyökkäyksiä) on iso kirjo mutta ehdottomasti suosituimmat ovat UDP:ta käyttävä NTP sekä sovellustasolla toimiva DNS. Esimerkiksi joulun Playstation-verkon hyökkäys käytti NTP-hyökkäystä. Heijastushyökkäyksessä kierrätetään hyökkäyksessä käytetyt paketit jonkin huonosti määritellyn palvelimen kautta, esimerkiksi huonosti määriteltyjä DNS-palvelimia on maailmassa miljoonia (Piscitello 2011).

Paketti lähetetään tällaiselle palvelimelle muokatulla lähdeosoitteella, lähdeosoite on hyökkäyksen oikea kohde. Palvelin vastaa kohteelle ja samalla paketin koko on moninkertaistunut huonosti määriteltyjen palveluiden takia. NTP-palvelun kohdalla paketin koko moninkertaistuu 556 kertaisesti eli jos yksi bottiverkon jäsenistä lähettää

palvelimelle megabitin edestä tavaraa, saa hyökkäyksen kohde 556 megabittiä liikennettä (Saarinen 2014, 17).

Protocol	Bandwidth Amplification Factor	Vulnerable Command
DNS	28 to 54	see: TA13-088A [1]
NTP	556.9	see: TA14-013A [2]
SNMPv2	6.3	GetBulk request
NetBIOS	3.8	Name resolution
SSDP	30.8	SEARCH request
CharGEN	358.8	Character generation request
QOTD	140.3	Quote request
BitTorrent	3.8	File search
Kad	16.3	Peer list exchange
Quake Network Protocol	63.9	Server info exchange
Steam Protocol	5.5	Server info exchange

KUVA 6. Heijastushyökkäyksen kertoimia taulukossa (Paganini 2014)

NTP-hyökkäyksessä käytetään hyödyksi palvelun vanhempia versioita joissa on vielä käytössä monlist-komento. Komento listaa kaikki tietokoneet jotka ovat käyttäneet palvelua ainakin kerran, listan maksimipituuden ollessa 600 osoitetta. Itse komento on vain pari sataa bittiä iso kun taas monlist-komennon palauttaman listan koko mitataan kilobiteissä. Hyökkäyksessä bottikoneet lähettävät monlist-komentoa turvattomille palvelimille lähdeosoite peukaloituna hyökkäyksen kohteeksi. Kohde saa palvelimilta ison määrän monlist-komennon tuottamia listoja ja kohteen verkon kaista tukkeutuu täysin (Acunetix 2014).

DNS-heijastushyökkäyksessä käytetään hyödyksi avoimiksi jätettyjä DNS-palveluja. Avoimeen DNS-palvelimeen voi ottaa yhteyttä mistä tahansa maailmalta vaikka itse DNS-palvelin hoitaisikin vain sisäverkon asioita. Palvelimelle lähetetään kysely jossa kysytään domainin kaikkia tietoja, jotka DNS-palvelin tietää domainista. Vastaus kyselyyn on ainakin 8-kertainen itse kyselyyn verrattuna, ja jos palvelimen maksimipakettikooksi on määritetty 4 kilotavua, on kerroin yli 60-kertainen. NTP:n tapaan nämä vastaukset suuntautuvat hyökkäyksen kohteelle, tukkien kaistan (Piscitello 2014).

DNS:n ja NTP:n ohella mainitsemisen arvoisia ovat CHARGEN- ja SNMP-protokollia käyttävät hyökkäykset sillä niiden suosio on ollut kasvamaan päin viime vuosina(Saarinen 2014, 16). Niiden toimintaperiaate on sama, pienikokoinen kysely palauttaa paljon isomman paketin muutettuun lähdeosoitteeseen. CHARGEN-protokolla kehitettiin jo 1983 ja sitä käytettiin todella harvoin kunnes sen

haavoittuvuus palvelunestohyökkäykseen keksittiin. Protokollan alkuperäinen tarkoitus on testata verkon käyttöä, esimerkiksi kaistan leveyttä. SNMP:llä (Simple Network Management Protocol) voidaan kysellä verkossa olevan laitteen tilaa. Palvelunestohyökkäyksien kannalta valitettavasti protokollan tuottama vastaus on paljon kyselyä isompi.

4.1.4 Ping of Death ja ICMP

Niin sanottu Ping of Death -hyökkäys on verkkoaikakauden klassikkoja. Aikoinaan hyökkäys suoritettiin lähettämällä ylisuuri ICMP-paketti vastaanottajalle, joka kaatoi käyttöjärjestelmän. ICMP-paketilla eli pingauksella on tarkoitus selvittää lähettäjän ja vastaanottajan välinen verkon viive. IP-paketin maksimikoon ollessa 65 535 bittiä, hyökkääjä muutti paketin ylisuureksi ja lähetti sen fragmentoituneena vastaanottajalle. Vanhat käyttöjärjestelmät yrittivät kasata fragmentteja paketeiksi ja paketin koon ylittäessä järjestelmien käsityskyvyn, ne kaatuivat. Tämä on kuitenkin korjattu jo ajat sitten, mutta sen johdannaisena syntyi ICMP Flood joka on nykyaikanakin käytetty hyökkäystyyli (Incapsula 2015).

ICMP flood on klassinen volyymihyökkäys. Kohteelle lähetetään valtava määrä viivettä kysyviä ICMP ping-paketteja. Tuloksena kohteen sekä ulos- että sisäänpäin tulevat yhteydet tukkeutuvat, koska kohde yrittää myös automaattisesti vastata näihin kyselyihin. ICMP-pakettien lähettäjän osoite on myös mahdollista naamioida, täydellisen anonyymiyden saavuttamiseksi.

4.2 Ohjelmistotason palvelunestohyökkäykset

Ohjelmistotason hyökkäykset ovat kasvattaneet suosiotaan suuresti viime vuosina. Tämän tason hyökkäyksissä hyökkääjän ja kohteen välinen yhteys on kokonaan niin sanotusti täydellinen, eli se toimii kuten mikä tahansa normaali kanssakäyminen

verkossa ja ruuhkapiikin ja palvelunestohyökkäyksen ero saattaa olla havaitsemattomissa.

Kohteelle lähetetään aidon näköisiä kyselyitä, esimerkiksi nettisivujen latauksia, mutta näillä kyselyillä on tarkoitus rasittaa itse palvelinta ja saattaa se toimintakyvyttömäksi tai vain hidastaa sen tasolla joka vaikuttaa oikeiden sivujen käyttäjien toimintaan. Usein itse verkon kaista riittää mutta kohdepalvelimen muisti tai prosessoriteho loppuu.

HTTP flood

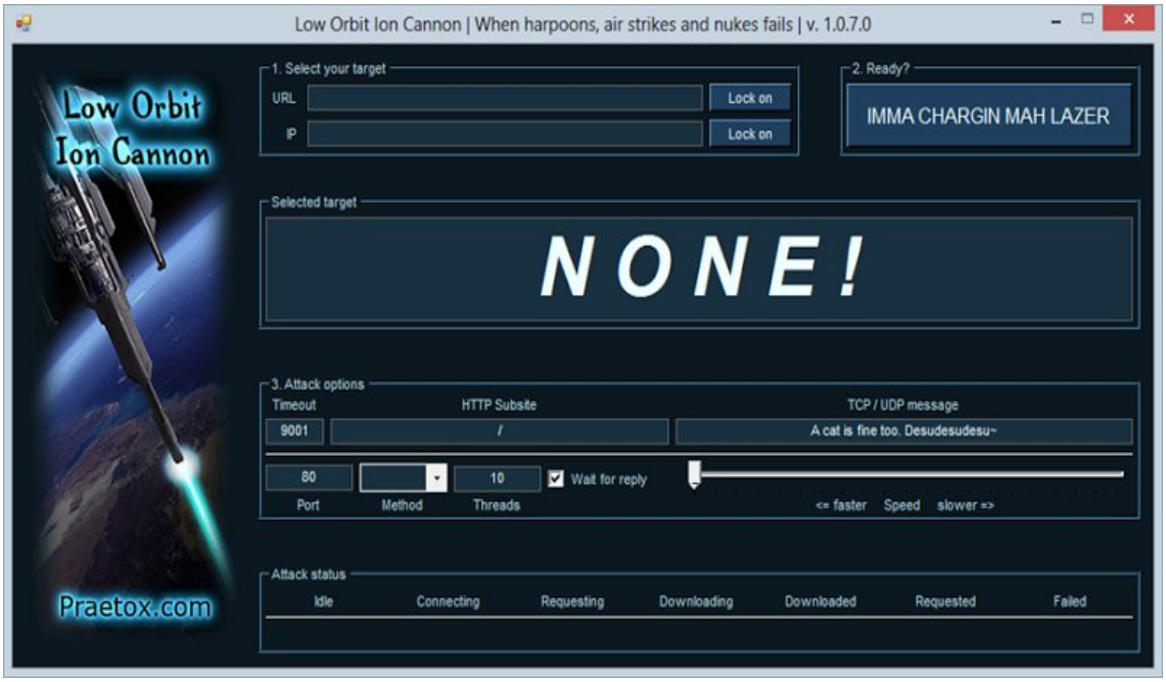
Ohjelmistotason hyökkäystyylejä on useita, verkon palveluista löytyy jatkuvasti heikkouksia joita käyttää hyväksi. Kuitenkin kestosuosikki ja yleisesti käytössä on HTTP flood, sen suorittamisen helppouden ja luonteensa ansiosta. Hyökkäyksessä verkkosivulle tai muulle http-protokallan palvelulle lähetetään massiivinen määrä HTTP-GET tai HTTP-POST kyselyjä, näillä kyselyillä käyttäjä ilmoittaa haluavansa ladata vaikka verkkosivuston jonkin osan, esimerkiksi kuvan (Radware 2015).

Vilkkaalle palvelulle tämä saattaa näyttää vain ruuhkapiikiltä mikä hankaloittaa toimia sitä vastaan. Hyökkäyksessä hyökkääjä ei vain odota kyselyihin vastausta vaan tunkee kyselyä jatkuvalla syötöllä, ja taitava hyökkääjä kohdistaa kyselynsä ympäri palvelua, naamioiden sitä vieläkin aidommaksi käytöksi.

4.2.1 Ohjelmistot

Palvelunestohyökkäyksiä varten löytyy Googlen kautta ohjelmistoja todella helposti ja YouTubessa on jopa videoita, joissa käydään niiden käyttöä läpi askel askeleelta. Useimmat ohjelmistot perustuvat volyymiin tai jonkun verkkopalvelun heikkouteen, esimerkiksi nettisivujen ylläpitoon tarkoitetun Apachen heikkouksiin löytyy parissa sekunnissa monta ohjelmaa. Googlella löytyvät ohjelmistot ovat käytön helppouden takia niin sanotusti amatöörien tavaraa eli niitä suosivat haktivistien kaltaiset käyttäjät.

Tunnetuin työkalu lienee LOIC eli Low Orbit Ion Cannon, tunnetuksi sitä on tehnyt Anonymous-ryhmä. LOIC:n käyttöliittymä on esitetty kuvassa 6. Sen ulkoasu ja käyttö on hiottu mahdollisimman helppokäyttöiseksi, mahdollistaen täysin amatöörien toiminnankin. Työkalulla ryhmä on suorittanut protestihyökkäyksensä esimerkiksi Visaa vastaan. Se perustuu volyymiin eli ryhmä kerää ison joukon ihmisiä, jotka pommittavat kohdetta yleensä HTTP-GET-kyselyillä, kysely paljastaa samalla jokaisen osallistujan IP-osoitteen mutta ryhmäläiset toivovat hukkuvansa massaan, tai voivansa väittää tietokoneidensa olleen saastuneita jos kiinnijääminen uhkaa (Hunt 2013).



KUVA 7. LOIC-käyttöliittymä (Hunt 2013)

Käyttäjän tarvitsee vain määrittää kohteen nettisivujen yleinen osoite tai IP-osoite, valita hyökkäyksessä käytettävä protokolla HTTP:n, UDP:n ja TCP:n kesken, ja painaa nappia hyökkäyksen aloittamiseksi.

5 HYÖKKÄYKSILTÄ SUOJAUTUMINEN JA VAHINKOJEN MINIMOINTI

Palvelunestohyökkäyksiltä suojautumiseen kannattaa suhtautua samoin kuin tietoturvallisuuteen yleensä. Ajattelussa ei tule keskittyä hyökkäyksen pysäyttämiseen vaan ennaltaehkäisyyn. Tietoturvan perusperiaatteilla eli pitämällä laitteet, ohjelmistot

ja palvelut ajanmukaisina ja poistamalla turhat palvelut ja protokollat pääsee jo pitkälle.

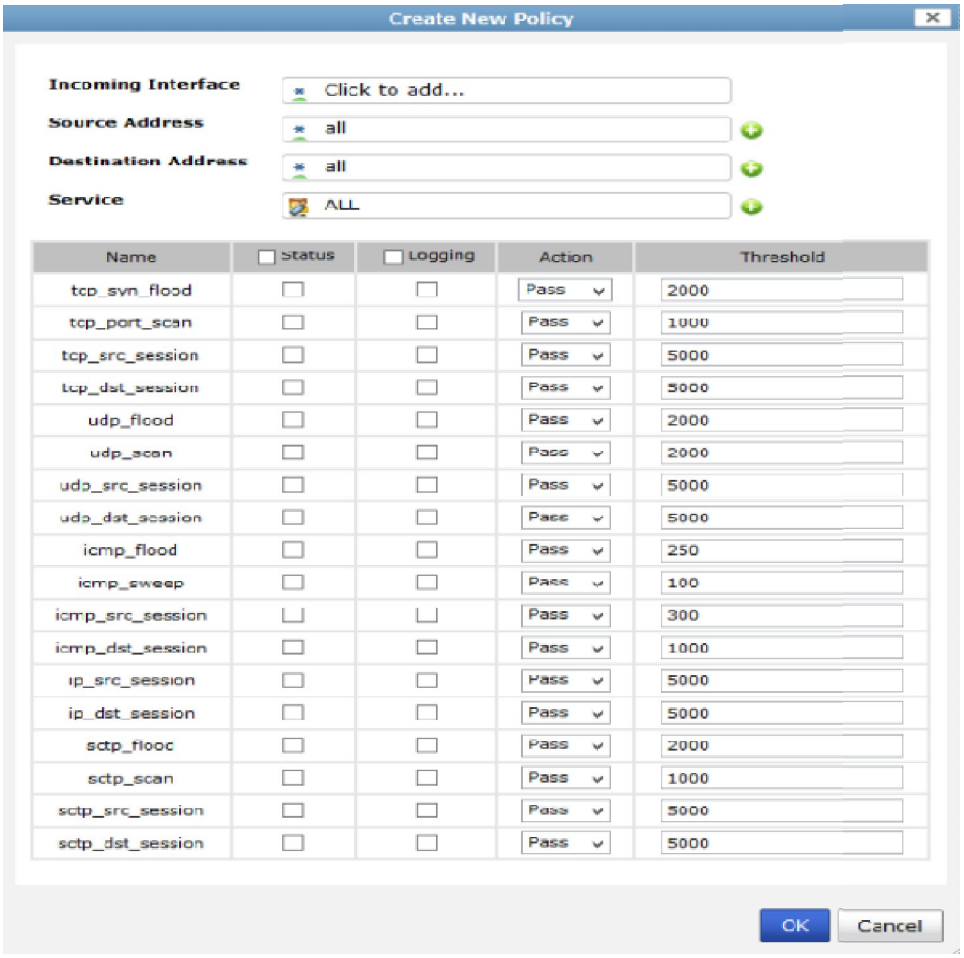
Esimerkkinä erittäin tehokas NTP-heijastushyökkäys, jonka käyttö olisi mahdotonta jos NTP-palvelun versio olisi päivitetty palvelimissa ympäri maailmaa. Poistamalla CHARGEN-protokollan käytöstä ei omaa palvelinta voitaisi käyttää myös CHARGEN-heijastushyökkäyksessä. Verkosta löytyy myös palveluja DNS-palvelimen testaukseen, esimerkiksi http://openresolver.com/:ssa voi testata oman domainin DNS-palvelimen avoimuutta ja näin varmistaa, ettei oma palvelin ole mukana tuhoisissa DNS-hyökkäyksissä.

5.1 Palomuurit

Markkinoilla on paljon Anti-DDoS nimillä myytäviä palomuureja, joiden erikoisalaa on normaalien palomuuritoimintojen lisäksi erikoistuminen palvelunestohyökkäyksien estoon. Palomuuri tulisi asettaa sisäverkon ja ulkomaailman väliin suodattamaan kaiken ulkoa tulevan liikenteen. Ohjelmistoilla voi suojautua useimpia protokollatason ja volyymitason hyökkäyksiä vastaan. Palomuurilla voi sulkea verkkonsa kokonaan ulkopuolisilta ICMP ping-kyselyiltä, jolloin Ping of Death ja ICMP flood-tyyliset hyökkäykset estetään jo palomuurin kohdalla.

UDP flood, TCP SYN flood ja HTTP flood-hyökkäyksiä palomuurit kitkevät avattujen yhteyksien perusteella. Hajauttamattomia palvelunestohyökkäyksiä vastaan palomuuri on käytännössä läpäisemätön, palomuurin voi asettaa estämään yhteydet IP-osoitteesta joista tulee epänormaali määrä avattuja yhteyksiä yhteensä tai liian monta yhteyden avausta sekunnissa.

Palomuureissa voi myös olla ominaisuus, joka estää paketit joiden lähdeosoitetta on peukaloitu. Lähdeosoitteen muuttamista käytetään melkein jokaisessa palvelunestohyökkäystyylissä oman osoitteen salassapitoon ja heijastushyökkäyksissä massiivisen tietotulvan luomiseen, tällä ominaisuudella varmistaakin, ettei omasta verkosta lähde tietoa tekaistulla lähdeosoitteella. Kuvassa 8 on esitetty esimerkkipalomuuriin DoS-suojausominaisuuksia.



KUVA 8. FortiGate-laitteen DoS-suojan asetuksia (FortiNet)

Palomuurin ominaisuuksia voi myös hoitaa reitittimellä, tosin todella paljon yksinkertaisemmin. Esimerkiksi ICMP-pakettien tulon verkon ulkopuolelta voi estää kokonaan, mutta esimerkiksi HTTP floodia vastaan reititin on aseeton, sillä hyökkäys vaikuttaa sille normaalilta HTTP-liikenteeltä. DoS-hyökkäyksiä ehkäisevä palomuuri hidastaa verkkoa hieman enemmän kuin normaali palomuuri, sillä se käy läpi kaiken liikenteen joka sen läpi kulkee.

Black holing

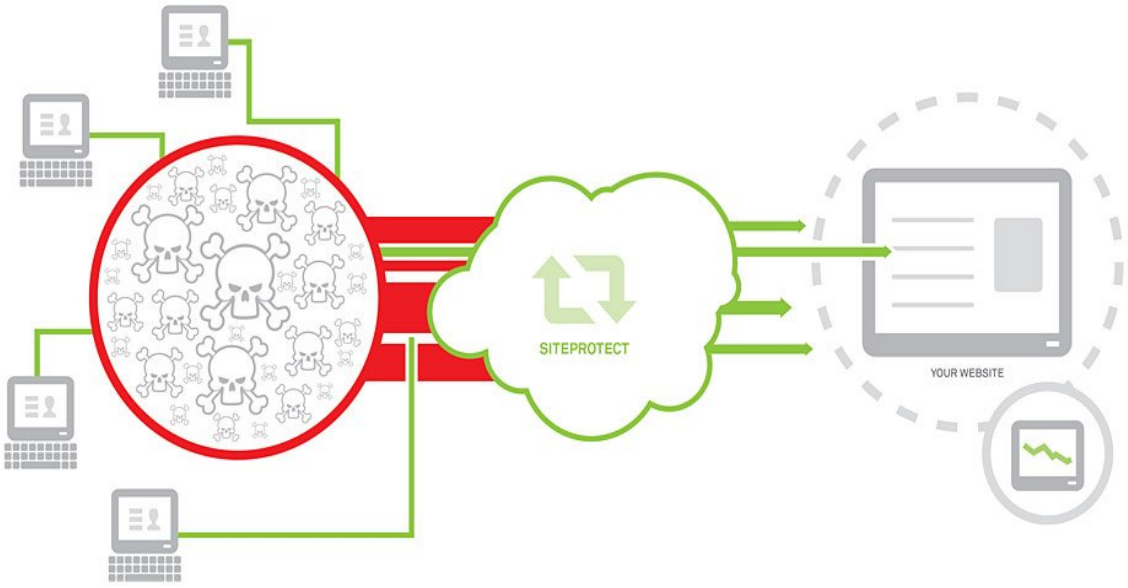
Palomuurit ja reititinsäädöt toimivat loistavasti palvelunestohyökkäystä vastaan, mutta kun verkkoon kohdistuukin hajautettu hyökkäys, ollaan ongelmissa. Hyökkäysdataa tulee monesta eri osoitteesta ja mahdollisesti monesta eri maista eli IP-osoitteen perusteella liikenteen estäminen ei enää auta. Vaikka hyökkäys olisi alkeellinen, esimerkiksi ICMP flood, voi se olla hajautettuna niin massiivinen, ettei kaista riitä tai

palomuurin ja reitittimen prosessointiteho ei enää riitä. Koska hyökkäysliikenne tulee oman verkon ulkopuolelta, vaikuttaa se palveluntarjoajan ja jopa maan verkon toimintaan, jos hyökkäys on massiivinen.

Isoissa hajautetun hyökkäyksen tapauksissa on turvauduttu niin sanottuun black holing-metodiin eli kohde irrotetaan ulkoverkosta lisävahinkojen välttämiseksi. Palveluntarjoajan kanssa voi myös neuvotella omaan verkkoon tulevan liikenteen kuristamista jotta muihin asiakkaisiin kohdistuva vaikutus pienenisi. Tämä ei missään nimessä ole kunnollinen tyyli hoitaa hyökkäykset, mutta joskus välttämätön.

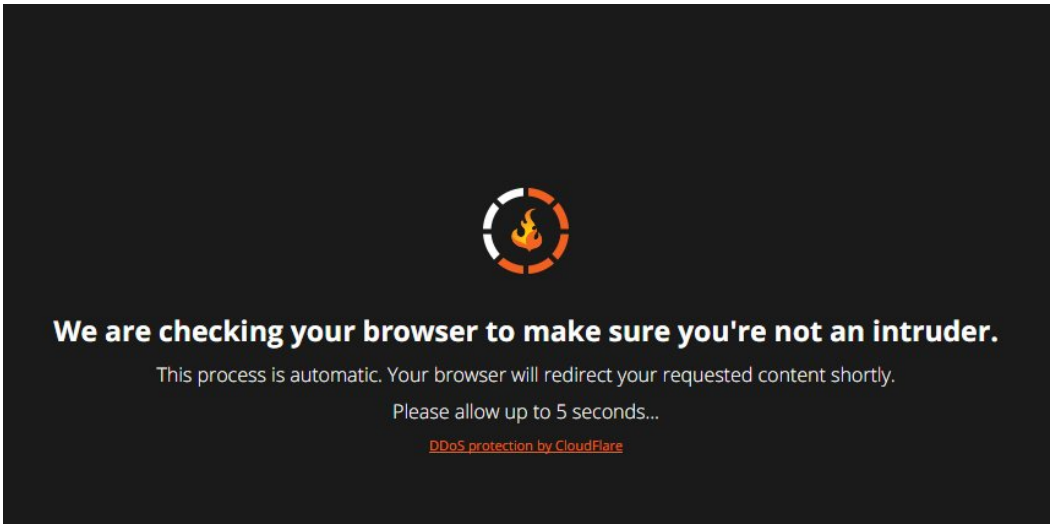
5.2 Puolustus pilvessä

Jos organisaation kaista tai laitteiden teho ei tunnu riittäviltä hyökkäystä varten, voi turvautua pilvipohjaisiin puolustusjärjestelmiin. Puolustusjärjestelmässä kaikki verkkopalvelun ja käyttäjien välinen liikenne kulkee pilvessä toimivan puolustuksen läpi. Pilvipalveluita tarjoavilla yhtiöillä on pätevät laitteet sekä hyökkäyspakettien suodattamiseen että luultavasti isompi verkkokaista ja hyökkäystä paremmin kestävät laitteet. Käytännössä siis hyökkäyksestä selviäminen ulkoistetaan pilvipalvelua tarjoavalle yhtiölle. Näitäkin pilvipalveluja on saatu polvilleen, mutta kyseessä ovat olleet todella massiivisiset hyökkäykset. Pilveä käyttävät palvelut ovat hieman hitaampia kuin normaalisti koska kaikki liikenne kulkee ja suodattuu pilvipalvelun läpi.



KUVA 9. Pilvipalvelupuolustus-esimerkki jossa Siteproject-palvelu suodattaa bottiverkon hyökkäystä (Neustar 2015)

Kuvassa 9 on esitetty tällaisen pilvipalvelun toimintaperiaate. Kaikki hyökkääjiltä lähtevä liikenne kulkee tarkistettavaksi Siteproject-palveluun, ja läpi pääsee vain murto-osa paketeista.



KUVA 10. Pilvipalvelu tarkistaa sivustolla suoritettuja hakuja (Curse 2015)

Kuvassa 10 CloudFlare-pilvipalveluyhtiön DDoS-suoja käytännössä www.curse.com -sivustolla. Käyttäjän suorittaessa haun sivustolla, CloudFlaren palvelu tarkistaa että haun kyselijä on aito käyttäjä, eikä raskaita hakukyselyjä sarjatulella laukova saastunut botti-tietotokone.

5.3 IDS / IPS

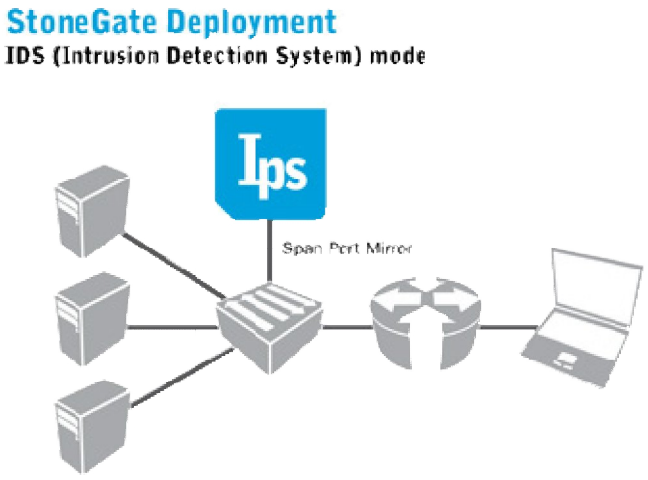
Organisaation verkon käyttöä ja palvelimien kuormitusta tulisi seurata ja saada selvä kuva, kuinka resursseja käytetään normaalisti sekä ruuhkapiikkien aikaan. Seuranta tulisi suorittaa ohjelmalla tai ohjelmilla, joissa näkyvät yhteyksissä käytetyt IP-osoitteet ja protokollat. Kun verkon normaali käyttäytyminen on tiedossa ja vika-ilmoituksia alkaa käyttäjiltä saapua, on helppo havaita jos kaistaa tai palvelimien

resursseja käyttää jokin pahantahtoinen taho, esimerkiksi TCP SYN-hyökkäyksessä seurantaohjelma täyttyisi TCP-yhteyksien avauksista.

Seurannan voi suorittaa myös automaattisesti palomuuri joka kerää verkon käytöstä tietoja kunnes sillä on kuva kuinka resursseja normaalisti ja ruuhkaisina hetkinä käytetään. Jos liikenne ylittää ruuhkapiikinkin, varoittaa se ylläpitäjää mahdollisesta hyökkäyksestä.

5.3.1 IDS

IDS eli Intrusion Detection System on yleensä joko verkon ulkolaidalla tai palomuurin ja sisäverkon väliin sijoitettu laite. Ulkolaidalle sijoitettuna se tutkii koko verkon liikenteen, palomuurin jälkeen sijoitettuna se tutkii sijoitetun liikenteen. Ulkolaidalle sijoitettuna se saattaa hidastaa verkkoliikennettä, koska laite joutuu tutkimaan koko verkon suodattamattoman liikenteen, mutta tällä ratkaisulla voidaan kartoittaa koko verkon liikenne ennen kuin reititin ja palomuuri pääsevät suodattamaan sitä. Tällainen kartoitus voi olla hyödyllistä jos halutaan tietää esimerkiksi kuinka usein hyökkäysyrityksiä tapahtuu (Infosec 2013).



KUVA 11. IDS (kuvassa Ips) sijoitettuna reitittimen jälkeen tutkimaan verkon liikennettä, verkon koneet vasemmalla, internet oikealla (Stonesoft 2015)

IDS:n päätoiminnot ovat tunnettujen virusten ja matojen tunnistaminen sekä verkon monitorointi. Palvelinestohyökkäyksiä vastaan se tutkiin verkon käyttöä

organisaatiossa ja antaa varoituksen jos se havaitsee jotain erikoista, esimerkiksi epänormaalin määrän HTTP GET-kyselyjä. Lisäksi IDS:n voi asettaa toimimaan tunnettujen hyökkäystyylien perusteella, esimerkiksi iso määrä TCP SYN-kyselyjä laukaisisi hälytyksen vaikka kyseessä sattuisi olemaan vain ruuhkapiikki.

Molemmissa systeemeissä on omat heikkoutensa, verkon käyttäytymiseen perustuva systeemi antaa helposti virhehälytyksiä jos organisaation verkkopalvelut kokevat odottamatonta ruuhkaa, esimerkiksi uutisen tai verkkopalvelun päivityksen takia. Hyökkäystyylien tunnistavalle systeemille taas on vaikea asettaa kynnys jolloin se päättää, ettei kyseessä ole ruuhka vain hyökkäys palvelua kohtaan.

IDS:llä on monia heikkouksia, kuten väärien hälytysten antaminen sille erikoisten verkkotapahtumien takia, lisäksi ne pudottavat paketteja jos liikennettä on laitteelle liikaa. Myös kaikki salattu liikenne kuten VPN-yhteydet menevät laitteesta läpi ilman tarkistusta.

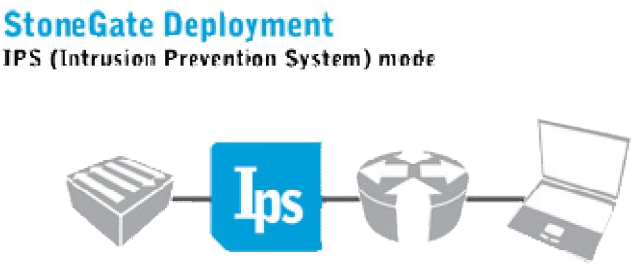
5.3.2 IPS

IDS antaa pelkkiä hälytyksiä, minkäänlaista suojaa se ei tarjoa itsessään, siksi on kehitetty IPS eli Intrusion Prevention System. IPS yhdistää IDS:n ja palomuurin ominaisuuksia ja lisää muuta tietoturvaa kuten matojen, virusten ja verkon tunkeutumisyritysten torjumista. Se voikin olla myös integroituna palomuuriin.

IPS:n toimintaperiaate on periaatteessa sama kuin IDS:n, IPS:n vain tekee hälytyksen lisäksi myös vaarallisten pakettien torjumisen. Palvelunestohyökkäysten tapauksessa se voi estää hyökkäävät yhteydet, aivan kuten palomuuri tekisi. Sijoitusperiaatteet ovat samat kuin IDS:llä, tosin IPS:n sijoittamista verkon päätelaitteiden ja palvelimien väliin kannattaa harkita, sillä madot ja virukset voivat lähteä liikkeelle myös verkon sisällä.

IPS:n suurin etu on keskitetty tietoturva, sama laite tai laitteet, riippuen verkon koosta, hoitavat palomuurin, virustorjunnan ja tunkeutumisyritysten toimintoja. Tämä tekee

tietoturvan pitämisestä ajan tasalla helpompaa ja nopeampaa, päivitettävänä on yksi laitetyyppi monen eri laitteen ja ohjelmiston sijaan.



KUVA 12. IPS, kuvassa nimellä Ips (Stonesoft 2015)

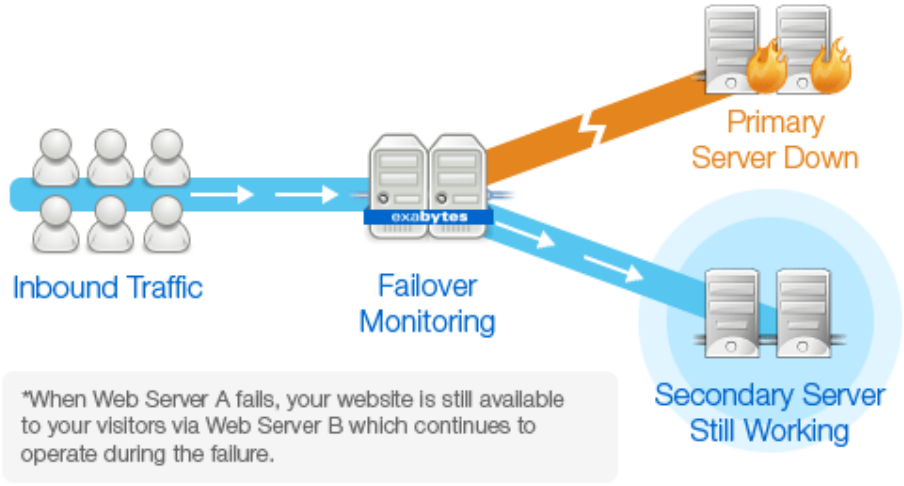
Kuvassa 11 IPS on sijoitettu reitittimen ja sisäverkon kytkimen väliin, joten se tutkii ja suodattaa kaikki paketit, jotka reititin on päästänyt läpi verkkoon.

5.4 Hajauttaminen

Hajauttaminen ja palvelujen kuorman jakaminen on tärkeä keino pitää verkko toiminnassa vaikka se olisikin hyökkäyksen alhainen. Kuorma yleensäkin pitäisi pyrkiä mahdollisimman keveänä, esimerkiksi suurin osa nettisivustoista on raskaampia kuin ne optimoimalla voisivat olla.

Kuorman jakamisella tarkoitetaan palvelun tai palveluiden hajauttamista eri laitteille, jotta palvelimet eivät ole jatkuvasti kovan rasituksen alaisia. Pelkästään hyvin jaettu kuorma ja keveät palvelut auttavat voittamaan heikon palvelunestohyökkäyksen, kaista ei täyty tai laitteiden resurssit eivät lopu kesken.

Jos organisaation verkon ylläpito on kriittinen, eli alhaalla oloa ei sallita tai se johtaa rahan menetyksiin, auttaa palveluiden ja laitteiden replikointi. Replikointipalvelin on varmuuskopio työtä tekevästä palvelimesta ja se aloittaa työt siinä vaiheessa kun itse pääpalvelin on hyökkäyksen alainen ja toimintakyvytön.



KUVA 13. Esimerkki varapalvelimesta (Exabytes Clustered Hosting 2015)

Sama periaate toimii myös reitittimissä tai verkon palomuurissa, jos pääreititin menee tukkoon tietotulvasta, ottaa varareititin ohjat ja yrittää auttaa tulvan ohjauksessa. Jos verkon kaista on kovilla, voidaan ottaa käyttöön myös eri verkossa sijaitsevat laitteet, tämä ratkaisu tosin alkaa jo todella kallis.

Kannattaa myös harkita palveluiden siirtämistä pilveen. Pilveen siirretty verkkosivu on kokonaan palvelua tarjoavan yhtiön vastuulla jos se joutuu hyökkäyksen kohteeksi. Samalla organisaation sisällä voidaan pitää varasivustoa, jolla voi paikata mahdollista pilven alhaalla oloaikaa. Pilveen vienti ei tosin ole kaikille ratkaisu, organisaation tietoja ei välttämättä haluta siirtää ulkomaiseen haltuun.

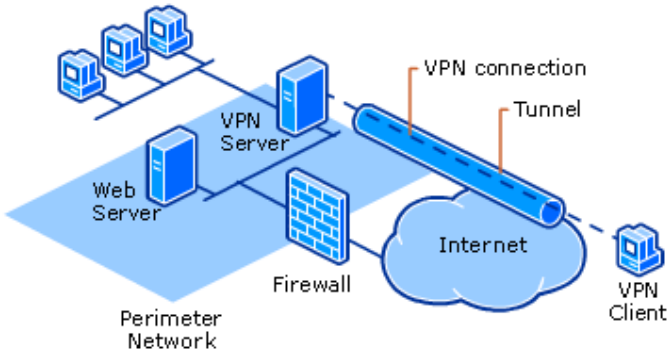
Hajauttaminen on ehdottomasti tehokkain keino taistelussa hyökkäyksiä vastaan. Kaikista suojautumiskeinoista huolimatta sinnikäs hyökkääjä tulee löytämään keinon päästä verkon kimppuun, mutta harvalla hyökkääjällä on resurssit hyökätä kaikkien hajautettujen palveluiden kimppuun.

5.5 Yksityishenkilöiden suojautuminen

Yksityishenkilökin on vaarassa joutua palvelunestohyökkäyksen kohteeksi. Jokaisen IP-osoite on lähtökohtaisesti muilta salassa mutta on olemassa tietoturvaltaan vajavaisia ohjelmistoja jotka vuotavat osoitteen kanssakäyttäjille. Pahin lähde lienee Skype, jossa voi selvittää käyttäjän IP-osoitteen vain tietämällä hänen käyttäjänimensä. Helpoin tapa välttyä hyökkäyksiltä on olla käyttämättä epävarmoja ohjelmia, mutta aina se ei ole mahdollista ja jo varmoiksi todetuista ohjelmista voi löytyä tietoturva-aukkoja.

Kun IP-osoite on vuotanut hyökkääjän tietoon, on pulassa josta ei pääse pois ennen kuin saa osoitteensa vaihdettua. Harvalla löytyy kotoa laitteet, joilla olisi mahdollisuutta puolustautua hyökkäystä vastaan. Kodin nettiliittymän kaista menee pienestäkin hajautetusta hyökkäyksestä jumiin.

Parhaimmat ratkaisut pitää oma osoite salassa ovat Virtual Private Network (VPN) ja Virtual Private Server (VPS). Molemmat palvelut laadukkaina maksullisia, ilmaisiakin löytyy mutta niillä ei kannata odottaa nopeaa toimivuutta. VPN:ssä tietokone ja VPN-palveluntarjoaja muodostavat keskenään tunnelin. Tunneli käyttää normaaleja tietoverkon osia ja kaistaa mutta sen sisältö on kahden keskeinen, muille verkon käyttäjille tunnelissa liikkuva data on salattua, myös IP-osoite.



KUVA 14. Esimerkki VPN-tunnelista internetin yli palomuurilla suojatulle palvelimelle (Microsoft 2009)

Mahdolliset hyökkääjät näkevät vain VPN-palveluntarjoajan IP-osoitteen, mutta palveluntarjoajalla on paljon paremmat resurssit ottaa vastaan hyökkäys kuin yksityishenkilöllä, lisäksi fiksu hyökkääjän yrittäjä hylännee idean saman tien turhana kun hän tajuaa että on hyökkäämässä palveluntarjoajaa vastaan. Suurin osa nettiliittymien palveluntarjoajista tarjoavat myös VPN-palveluja joten tunnelin pituudesta ei tule kohtuuttoman pitkä ja viiveet pysyvät mahdollisimman matalina, tosin salattu liikenne on aina hieman hitaampaa kuin normaali, tunnelin pituudesta riippumatta.

Toinen vaihtoehto VPS on hyvin samankaltainen kuin VPN. VPS on palvelin joka sijaitsee eri verkossa kuin sitä käyttävä henkilö. Käytännössä VPS vuokrataan joltain palvelulta, kuten Amazonilta. Ideana on muodostaa yhteys kotikoneen ja virtuaalipalvelimen välille salattuna, tämä onnistuu Secure Shellin (SSH) kaltaisilla salatun liikenteen protokollilla.

Lopputulos on sama kuin VPN:ssä, kotikoneen ja palvelimen välinen yhteys on salattua ja ulospäin näkyy vain VPS:n osoite ja mahdolliset hyökkäykset kohdistuvat sinne. Etuna virtuaalipalvelimen käytössä VPN:n sijaan on että salatun liikenteen voi säätää vain tietyille ohjelmille, kun taas VPN-yhteydessä kaikki liikenne on salattua. Esimerkiksi vain Skypen ohjaaminen VPS:n kautta vähentää muiden ohjelmien verkkoviivettä.

6 YHTEENVETO

Opinnäytetyön tavoite oli tutkia palvelunestohyökkäysten taustoja ja ottaa selville, kuinka ne toimivat, ketkä niitä tekevät ja miten niitä käytetään tietoverkkojen häirinnässä. Ne ovat ”muodissa” tällä hetkellä uutisia hyökkäyksistä saa lukea usein, hyökkäyshän on käytännössä aina huomiota herättävä. Ja usein hyökkäyksillä haetaan nimenomaan huomiota.

Taustatutkimuksen jälkeen tarkoituksena oli kartoittaa luotettavimmat ehkäisykeinot ja tavat jolla selvitä palvelunestohyökkäyksestä. Työhön ryhdyttiin tutkimalla ensin tietoverkon yleisimpiä protokollia ja verkon laitteiden osoitteenmuodostusta. Näiden esitteleminen oli välttämätöntä jos halutaan ymmärtää täydellisesti, kuinka useat palvelunestohyökkäykset toimivat teknisellä tasolla.

Taustatiedon jälkeen pureuduttiin palvelunestohyökkäyksiin yleisemmällä tasolla, mietittiin mihin ne pohjautuvat ja mitä ne oikeastaan ovat. Tekijöistä ja motiiveista mainittiin palvelunestohyökkäykset kybersodan aseena joista esimerkkejä tullaan luultavasti näkemään tulevaisuudessa jos ja kun kaksi kattavan tietoverkon omaavaa maata käyvät nokikkain. Motiivi- ja kohdeosion pääpaino oli kuitenkin amatööreissä ja usein kiusantekoon keskittyvässä hyökkäystoiminnassa, sillä se on varsinkin esitellyissä ympäristöissä lisääntynyt valtavasti viimeisen vuoden aikana.

Yleisimpien hyökkäystapojen osio käy tärkeimmät piirteet läpi organisaation tai henkilön verkon suurimpia uhkia palvelunestohyökkäysten saralla ja antaa mielestäni hyvän kuvan mihin valmistua, jos epäilee että voi joutua hyökkäyksen kohteeksi. Osioissa esiteltiin myös, kuinka yksinkertaista palvelunestohyökkäys on aloittelijallekin jos käytössä on hyökkäyksiin suunniteltu ohjelma.

Itse suojautumisosiossa käydään läpi lähinnä hyökkäyksen ennakointia ja valmistautumista, sillä yleensä läpi päässyt hyökkäys on todella vaikeata pysäyttää ilman verkon alas ajoa. Osiossa todetaan että nykyajan palveluhyökkäyksiä silmällä pitäen kehitetyt palomuurit pysäyttävät suurimman osan ei-hajautetuista hyökkäyksistä. Samalla esitellään puolustuksen vastuun siirtämistä kolmannelle osapuolelle eli pilvipalveluyrityksille.

Hyökkäyksen pysäyttämisen ollessa hankalaa on fiksua varautua hajauttamalla palveluja hyökkäyksestä selviytyäkseen, yleensä asettamalla varapalveluja eri osoitteisiin. Myös palvelujen vieminen pilveen on toimiva vaihtoehto, tosin tietosuojaseikat voivat estää pilven käytön. Palvelujen hajauttaminen on ehdottomasti tehokkain tapa selviytyä hajautetusta palvelunestohyökkäyksestä jos pilvipalvelut eivät ole optio, sillä hyökkääjät tuskin käyvät myös varapalvelujen kimppuun.

Yksityishenkilöille esitellään IP-osoitteen yksityisyyden tarpeellisuus hyökkäysten estossa. Parhaimmiksi keinoiksi estyä hyökkäyksiltä mainitaan VPN-yhteys ja virtuaalipalvelimen käyttö. Ne ovat niin sanotusti idioottivarmoja keinoja, IP-osoite ei voi vuotaa ulospäin mitenkään jos VPN- tai VPS-yhteys on onnistuneesti muodostettu. Opinnäytetyön tavoitteet täyttyivät hyvin, palvelunestohyökkäyksistä saa työstä tarvittavat taustatiedot ja suojautumiskeinoista hyvät apuviivat.

LÄHTEET

Goldman, David 2012. The Internet now as 340 trillion trillion addresses. WWW-dokumentti. http://money.cnn.com/2012/06/06/technology/ipv6/. Päivitetty 6.6.2012. Luettu 1.4.2015

Egevang, Kjeld. & Francis, Paul 1994. The IP Network Address Translator (NAT). WWW-dokumentti. https://www.ietf.org/rfc/rfc1631.txt. Päivitetty 18.5.1994. Luettu 1.4.2015.

Mockapetris, Paul. 1987. Domain names – Implementation and specification. WWW-dokumentti. https://www.ietf.org/rfc/rfc1035.txt. Ei päivitystietoja. Luettu 1.4.2015.

Transmission Control Protocol. 1981. DARPA. WWW-dokumentti. https://www.ietf.org/rfc/rfc793.txt. Päivitetty 16.10.1992. Luettu 1.4.2015.

Transmission Control Protocol. 2015. Wikipedia. WWW-dokumentti. http://en.wikipedia.org/wiki/Transmission_Control_Protocol. Päivitetty 2.5.2015. Luettu 26.3.2015.

TCP/IP Protokollat. 2001. WWW-dokumentti.

http://koti.mbnet.fi/mrin/kuvat/ip_sahke.gif. Päivitetty 31.1.2001. Luettu 1.4.2015.

Postel, Jon 1980. User Datagram Protocol. WWW-dokumentti.

https://www.ietf.org/rfc/rfc768.txt. Päivitetty 16.10.1992. Luettu 4.4.2015

Saarinen, Ari 2014. Onko yrityksesi dossattu? Tietokone 3, 12-21.

Glenny, Misha 2012. Hämärän markkinat: nettirosvot, nettipoliisit ja sinä. Helsinki: Tammi.

Markoff, John 2008. Before the Gunfire, Cyberattacks. WWW-dokumentti.

http://www.nytimes.com/2008/08/13/technology/13cyber.html. Ei päivitystietoja. Luettu 18.4.2015.

Hallamaa, Teemu 2015. Palvelunestohyökkäyksistä epäillyt vangittu. WWW-dokumentti.

http://yle.fi/uutiset/palvelunestohyokkayksista_epaillyt_vangittu/7900634. Päivitetty 31.3.2015. Luettu 24.4.2015.

Krebs, Brian 2013. DDos Attack on Bank Hid $900,000 Cyberheist. WWW-dokumentti. http://krebsonsecurity.com/2013/02/ddos-attack-on-bank-hid-900000-cyberheist/. Ei päivitystietoja. Luettu 27.4.2015.

Operation Payback. 2015. Wikipedia. WWW-dokumentti. http://en.wikipedia.org/wiki/Operation_Payback Luettu 27.4.2015. Päivitetty 25.4.2015. Luettu 27.4.2015.

Our Games. 2015. Riot Games. WWW-dokumentti. http://www.riotgames.com/our-games. Ei päivitystietoja. Luettu 28.4.2015.

Parkin, Simon 2014. Inside the mind of Derp, a hacking group with a taste for cyber chaos. WWW-dokumentti. http://www.theguardian.com/technology/2014/aug/28/derp-inside-hacking-group-cyber-attacks-phantomlord. Ei päivitystietoja. Luettu 28.4.2015

Atlas Summary Report. 2015. Arbor Networks. WWW-dokumentti. http://atlas.arbor.net/summary/dos. Päivitetty 7.5.2015. Luettu 30.4.2015.

CAPEC-495: UDP Fragmentation. 2015. CAPEC. WWW-dokumentti. http://capec.mitre.org/data/definitions/495.html. Päivitetty 4.12.2014. Luettu 30.4.2015.

UDP Flood. 2015. Incapsula. WWW-dokumentti. https://www.incapsula.com/ddos/attack-glossary/udp-flood.html. Ei päivitystietoja. Luettu 30.4.2015.

UDP Flood. 2002. CureLan. http://www.curelan.com/en/news/udp_flood.htm. Ei päivitystietoja. Luettu 13.5.2015.

Messer, James. The Danger of Decoy-Initiated SYN Floods. WWW-dokumentti http://www.networkuptime.com/nmap/page06-04.shtml. Ei päivitystietoja. Luettu 1.5.2015.

Woelk, Ben 2007. Avoiding the Botnet Snare. WWW-dokumentti. http://www.rit.edu/its/news/archive/07feb/botnet.html. Ei päivitystietoja. Luettu 1.5.2015.

Piscitello, David. WWW-dokumentti. https://www.watchguard.com/infocenter/editorial/41649.asp. Ei päivitystietoja. Luettu 2.5.2015.

Preventing NTP Reflection DDOS Attacks Based on CVE-2013-5211. 2014. Acunetix. WWW-dokumentti. https://www.acunetix.com/blog/articles/ntp-reflection-ddos-attacks/. Ei päivitystietoja. Luettu 2.5.2015.

SYN flood. 2015. Wikipedia. WWW-dokumentti. http://en.wikipedia.org/wiki/SYN_flood. Päivitetty 20.4.2015. Luettu 2.5.2015.

Paganini, Pierluigi 2014. Reflection DDoS Attacks Continue to be dangerous in Q3 2014. WWW-dokumentti. http://securityaffairs.co/wordpress/29055/cyber-crime/reflection-ddos-attacks-q3-2014.html. Ei päivitystietoja. Luettu 2.5.2015.

DDoS Attacks. 2015. Incapsula. WWW-dokumentti. https://www.incapsula.com/ddos/ddos-attacks/. Ei päivitystietoja. Luettu 3.5.2015.

HTTP Flood. 2015. Radware. WWW-dokumentti. http://security.radware.com/knowledge-center/DDoSPedia/http-flood/. Ei päivitystietoja. Luettu 4.5.2015.

Hunt, Troy 2013. What is LOIC and can I be arrested for DDoS'ing someone? WWW-dokumentti. http://www.troyhunt.com/2013/01/what-is-loic-and-can-i-be-arrested-for.html. Ei päivitystietoja. Luettu 4.5.2015.

DoS Policy. 2014. Fortinet. WWW-dokumentti. http://docs-legacy.fortinet.com/fmgr/50hlp/index.html#page/FMG_507_Online_Help/1100_Policies-_-Objects.15.41.html. Päivitetty 10.7.2014. Luettu 4.5.2015.

Neustar® SiteProtect. Intelligent DDoS Protection. 2015. Neustar. WWW-dokumentti. https://www.neustar.biz/resources/product-literature/ddos-mitigation-service-product-literature. Ei päivitystietoja. Luettu 5.5.2015.

Configure a Firewall for VPN Traffic. 2009. Microsoft. WWW-dokumentti. https://technet.microsoft.com/en-us/library/dd458955%28v=ws.10%29.aspx. Päivitetty 13.2.2009. Luettu 5.5.2015.

Stonesoft IPS. 2015. NDM. WWW-dokumentti. http://www.ndm.net/ips/solutions/stonesoft. Ei päivitystietoja. Luettu 10.5.2015.

Network Design: Firewall, IDS/IPS. 2013. Infosec Institute. WWW-dokumentti. http://resources.infosecinstitute.com/network-design-firewall-idsips/. Ei päivitystietoja. Luettu 10.5.2015.

Exabytes Clustered Hosting. 2015. Exabytes. WWW-dokumentti. http://exabytes.com.my/servers/clustered-hosting/. Ei päivitystietoja. Luettu 20.5.2015.

Curse. 2015. WWW-dokumentti. http://www.curse.com/. Päivitetty 20.5.2015. Luettu 20.5.2015.